Main elements of the Security System (100)

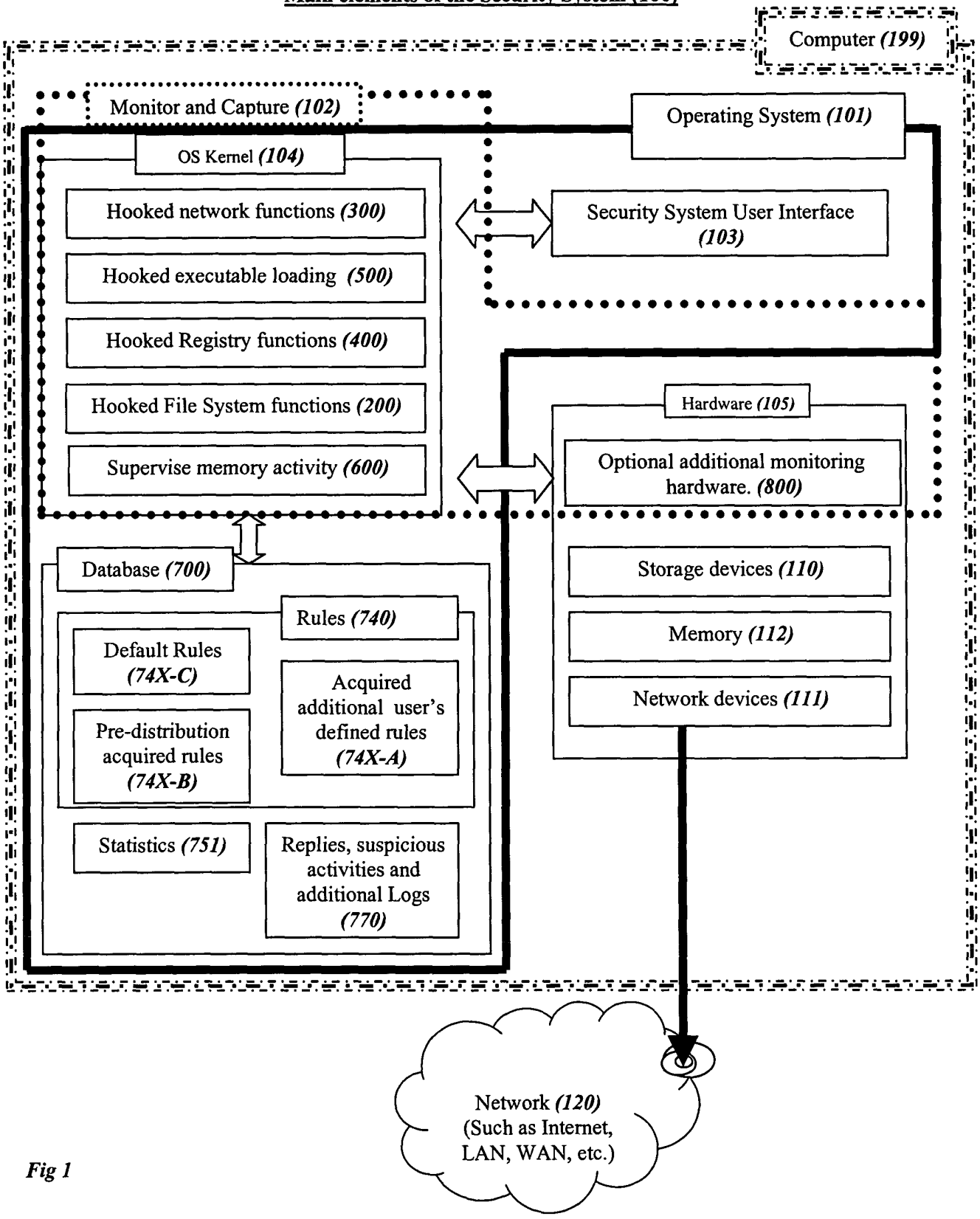


Fig 1

Interaction between Security System parts overview *(1100)*

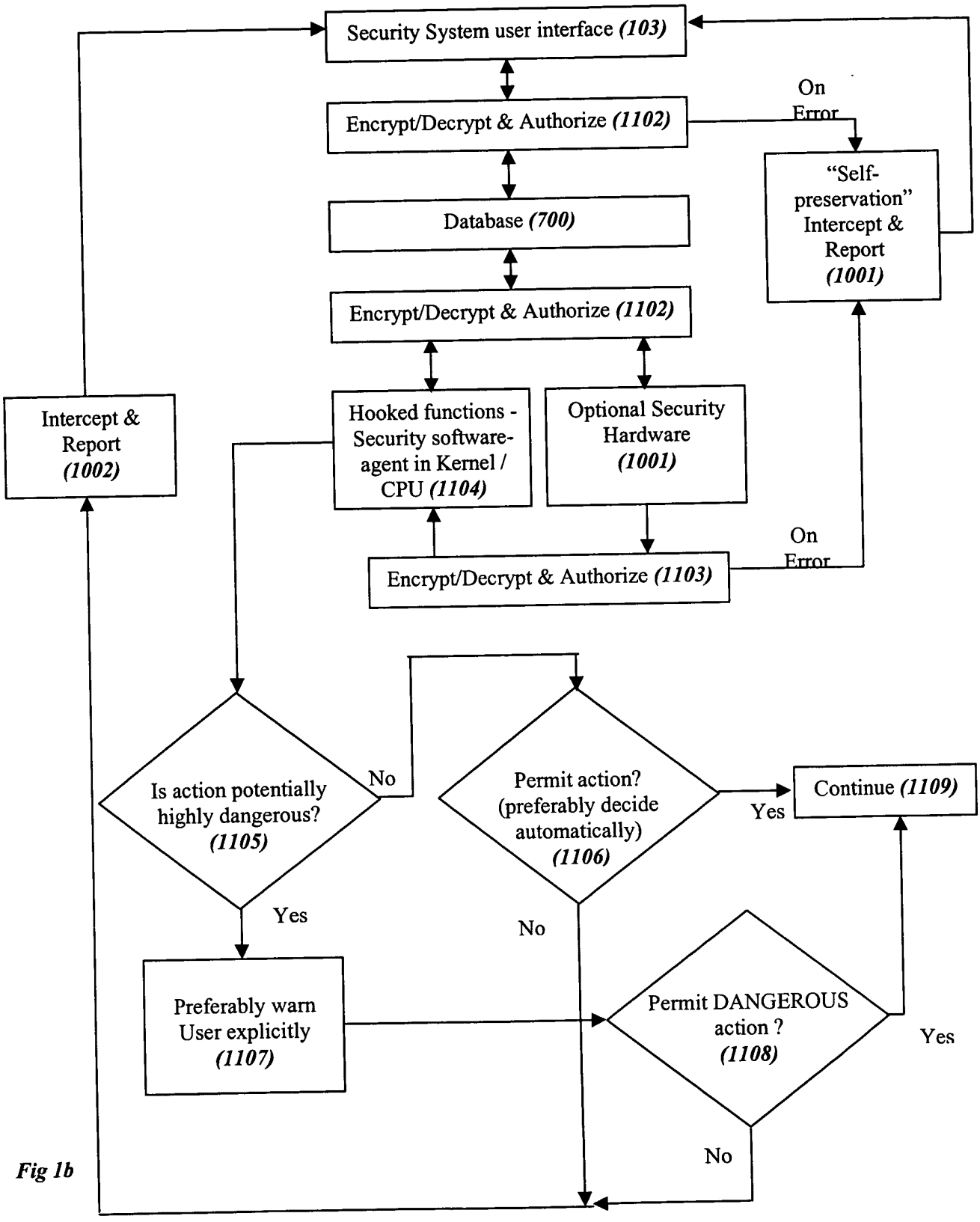


Fig 1b

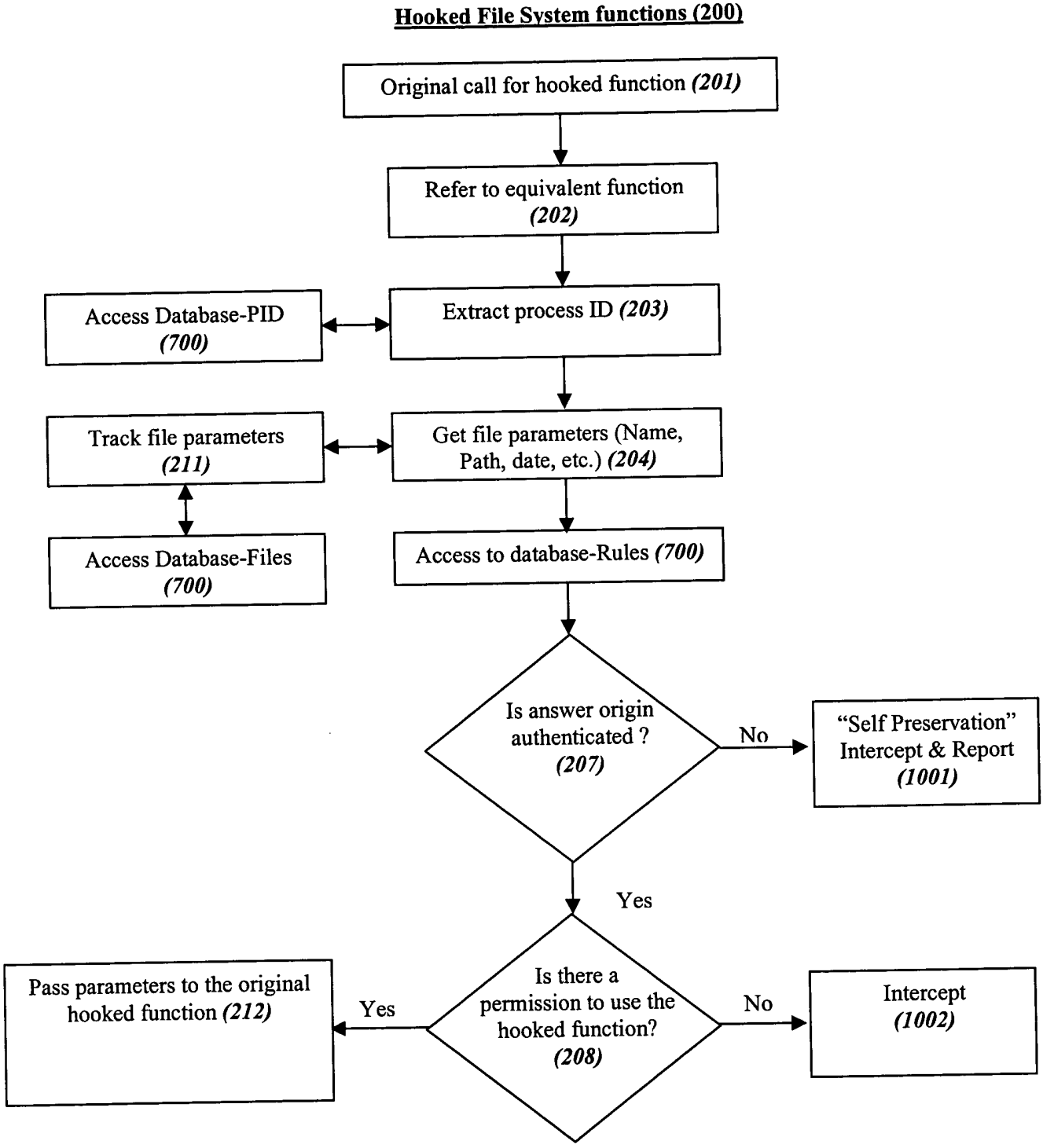

Hooked File System functions (200)
Original call for hooked function (201)
Refer to equivalent function (202)
Extract process ID (203)
Access Database-PID (700)
Get file parameters (Name, Path, date, etc.) (204)
Track file parameters (211)
Access Database-Files (700)
Access to database-Rules (700)
Is answer origin authenticated ? (207)
No
"Self Preservation" Intercept & Report (1001)
Yes
Is there a permission to use the hooked function? (208)
Yes
Pass parameters to the original hooked function (212)
No
Intercept (1002)

Fig 2

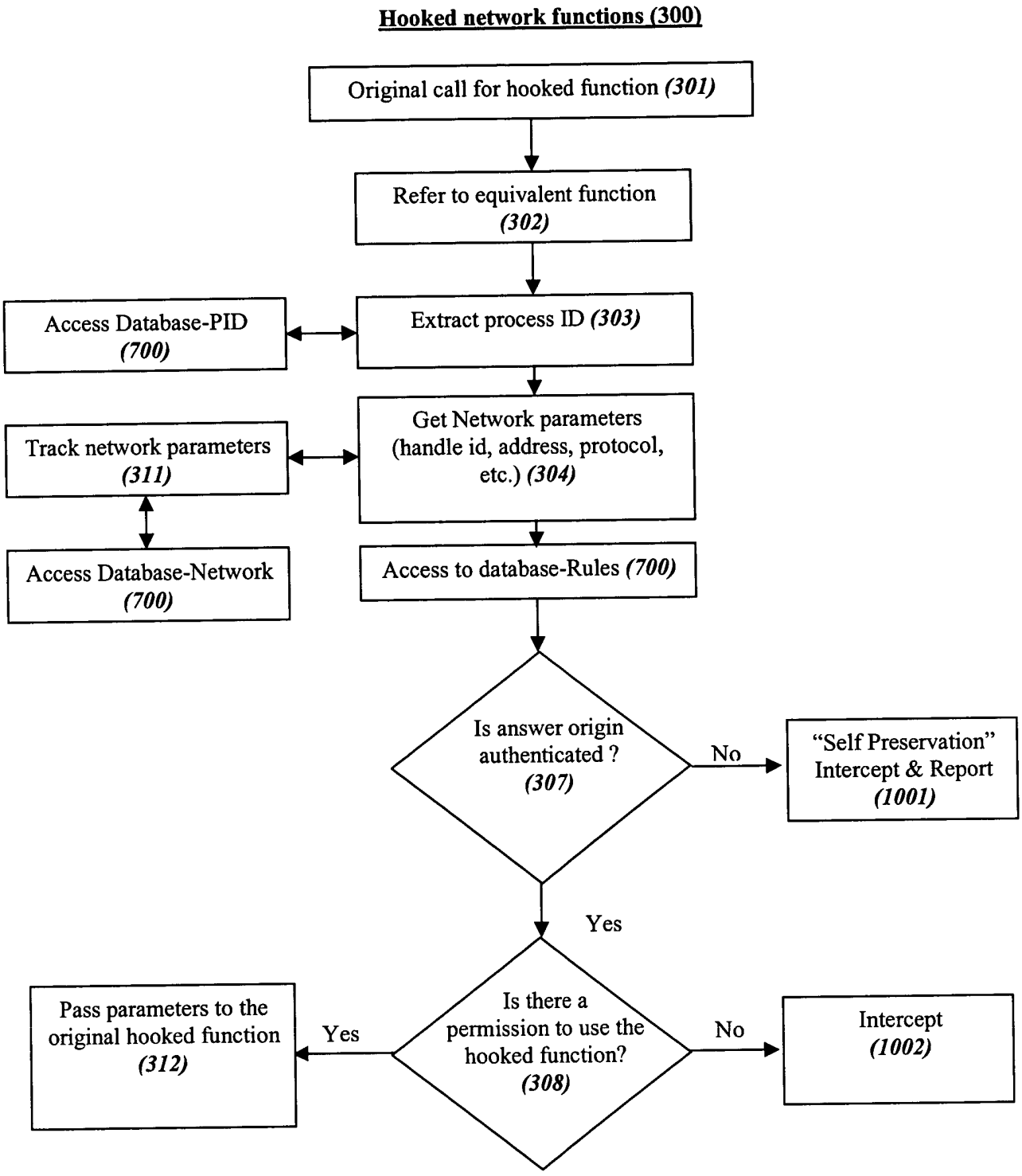

Hooked network functions (300)
Original call for hooked function (301)
Refer to equivalent function (302)
Extract process ID (303)
Access Database-PID (700)
Get Network parameters (handle id, address, protocol, etc.) (304)
Track network parameters (311)
Access Database-Network (700)
Access to database-Rules (700)
Is answer origin authenticated ? (307)
No
"Self Preservation" Intercept & Report (1001)
Yes
Is there a permission to use the hooked function? (308)
Yes
Pass parameters to the original hooked function (312)
No
Intercept (1002)

Fig 3

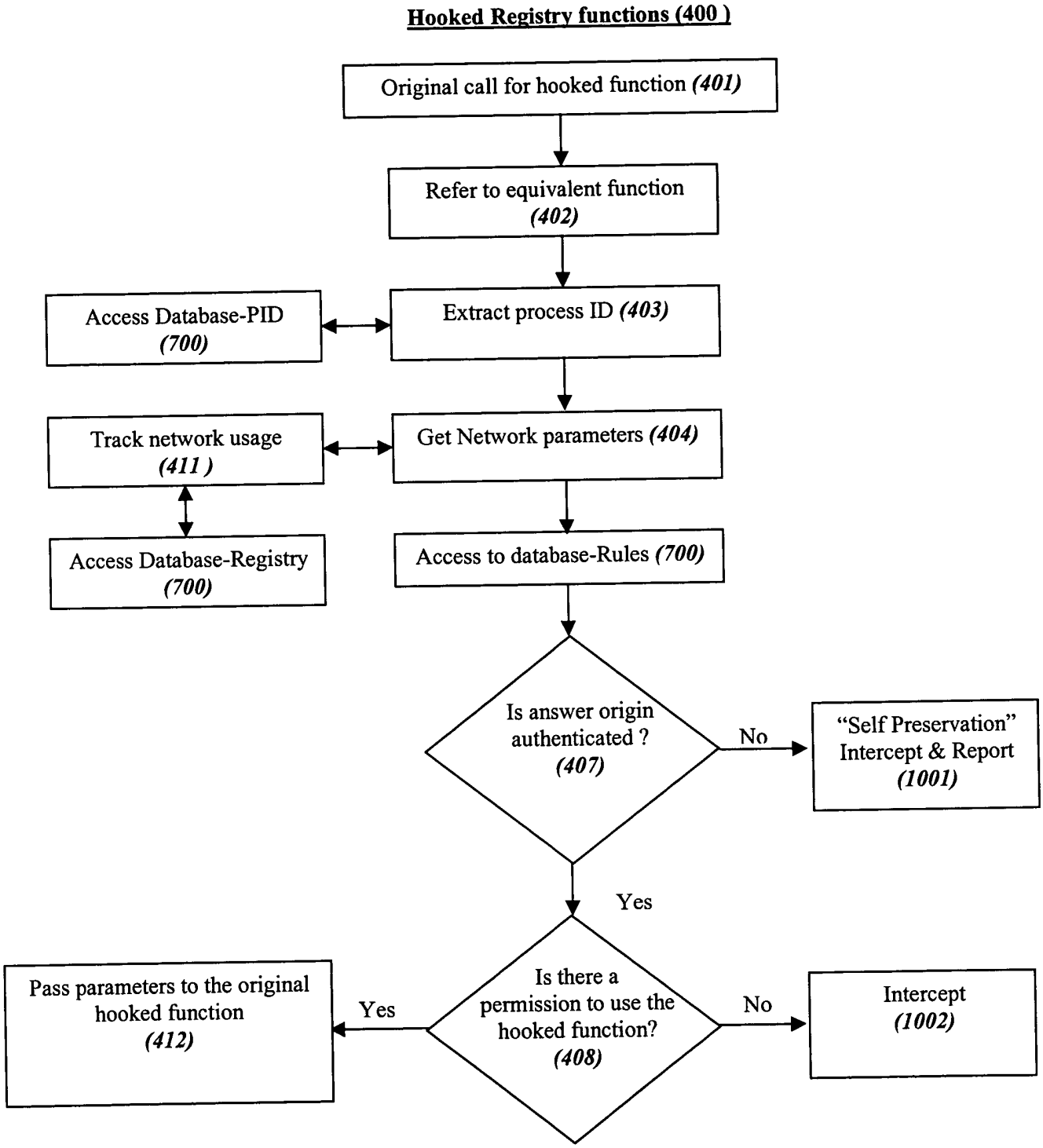

Hooked Registry functions (400)
Original call for hooked function (401)
Refer to equivalent function (402)
Access Database-PID (700)
Extract process ID (403)
Track network usage (411)
Get Network parameters (404)
Access Database-Registry (700)
Access to database-Rules (700)
Is answer origin authenticated ? (407)
No
"Self Preservation" Intercept & Report (1001)
Yes
Pass parameters to the original hooked function (412)
Yes
Is there a permission to use the hooked function? (408)
No
Intercept (1002)

Fig 4

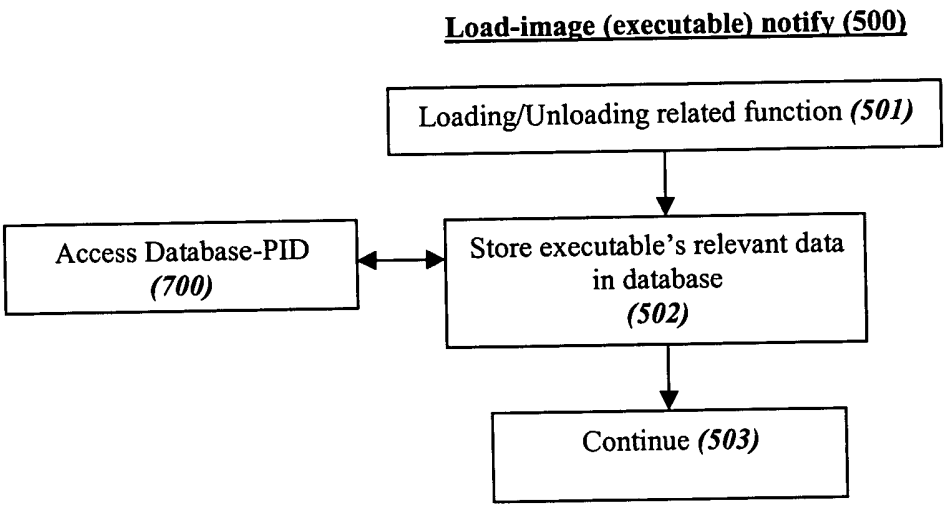

Load-image (executable) notify (500)
Loading/Unloading related function (501)
Access Database-PID (700)
Store executable's relevant data in database (502)
Continue (503)

Fig 5

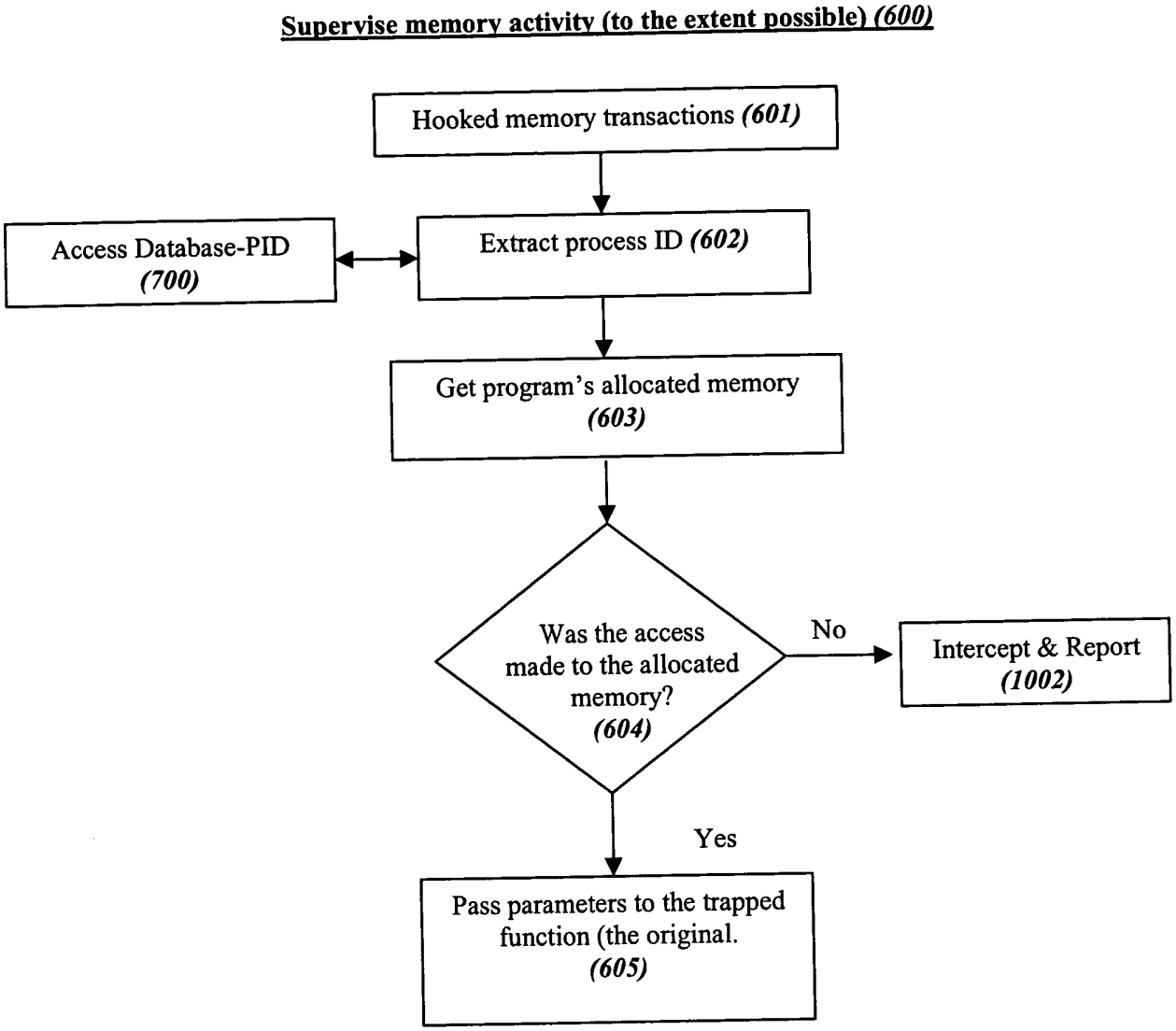

Supervise memory activity (to the extent possible) (600)
Hooked memory transactions (601)
Access Database-PID (700)
Extract process ID (602)
Get program's allocated memory (603)
Was the access made to the allocated memory? (604)
No
Intercept & Report (1002)
Yes
Pass parameters to the trapped function (the original. (605)

Fig 6

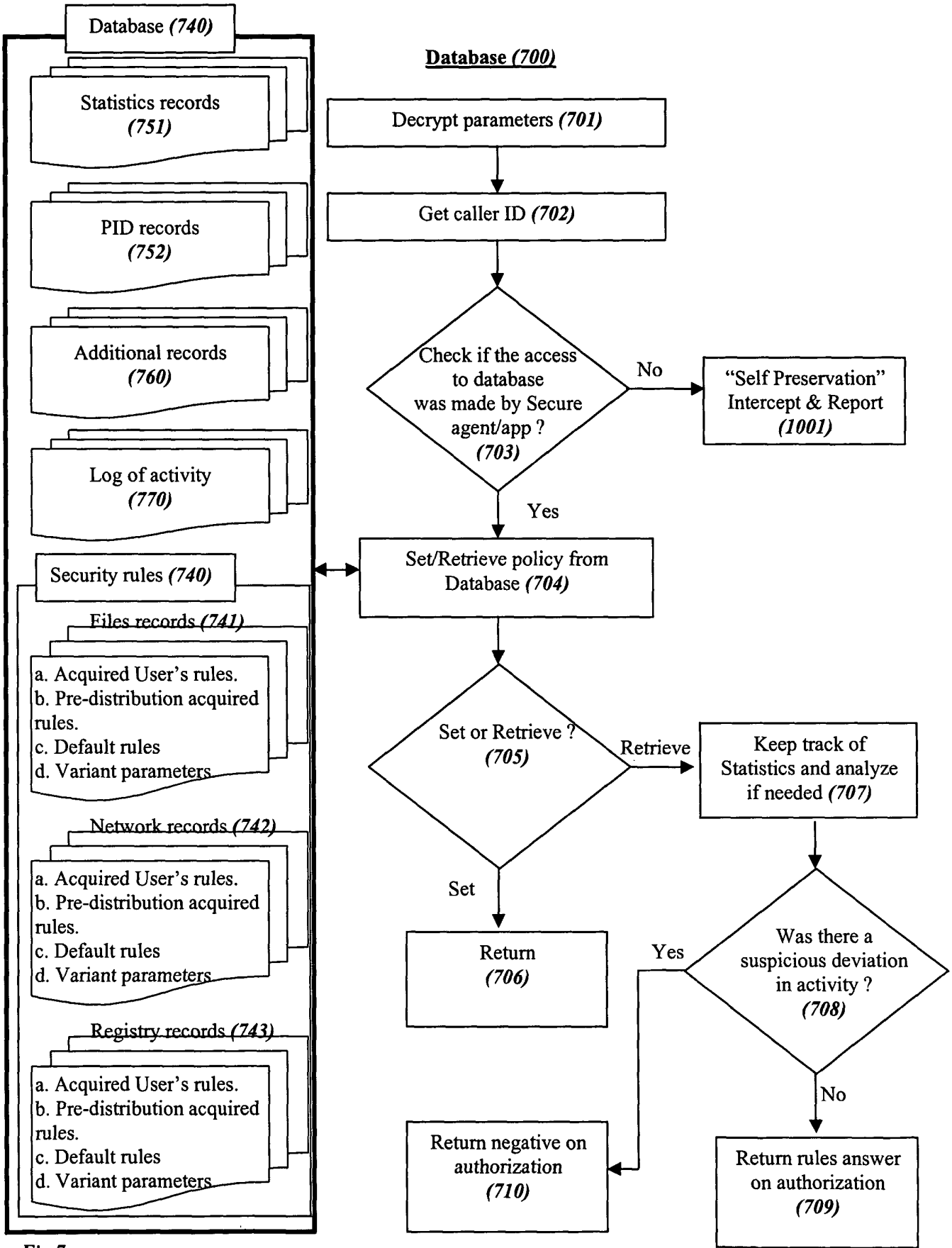

Database (740)
Statistics records (751)
PID records (752)
Additional records (760)
Log of activity (770)
Security rules (740)
Files records (741)
a. Acquired User's rules.
b. Pre-distribution acquired rules.
c. Default rules
d. Variant parameters
Network records (742)
a. Acquired User's rules.
b. Pre-distribution acquired rules.
c. Default rules
d. Variant parameters
Registry records (743)
a. Acquired User's rules.
b. Pre-distribution acquired rules.
c. Default rules
d. Variant parameters
Database (700)
Decrypt parameters (701)
Get caller ID (702)
Check if the access to database was made by Secure agent/app ? (703)
No
"Self Preservation" Intercept & Report (1001)
Yes
Set/Retrieve policy from Database (704)
Set or Retrieve ? (705)
Retrieve
Keep track of Statistics and analyze if needed (707)
Set
Return (706)
Was there a suspicious deviation in activity ? (708)
Yes
No
Return negative on authorization (710)
Return rules answer on authorization (709)

Fig 7

Optional additional monitoring hardware. *(800)*

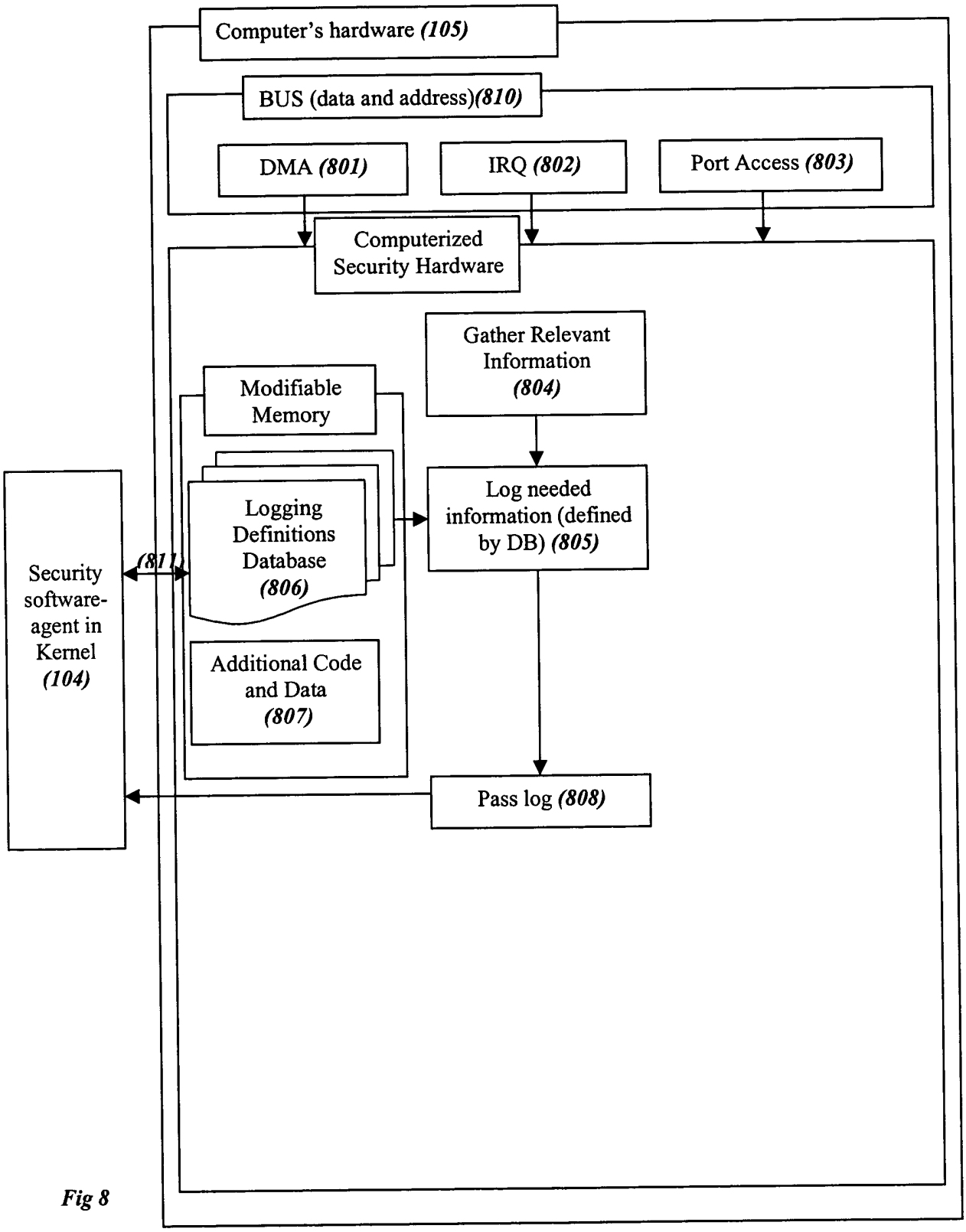


Fig 8

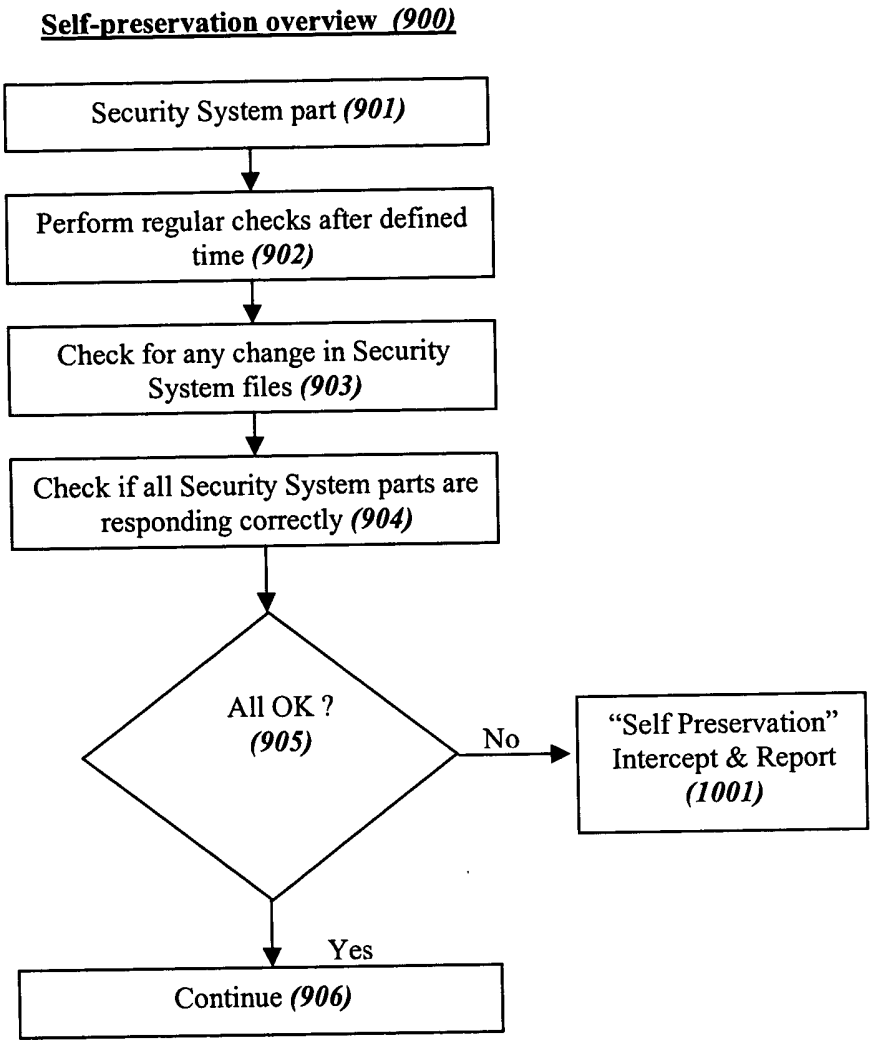

Self-preservation overview (900)
Security System part (901)
Perform regular checks after defined time (902)
Check for any change in Security System files (903)
Check if all Security System parts are responding correctly (904)
All OK ? (905)
No
"Self Preservation" Intercept & Report (1001)
Yes
Continue (906)

Fig 9

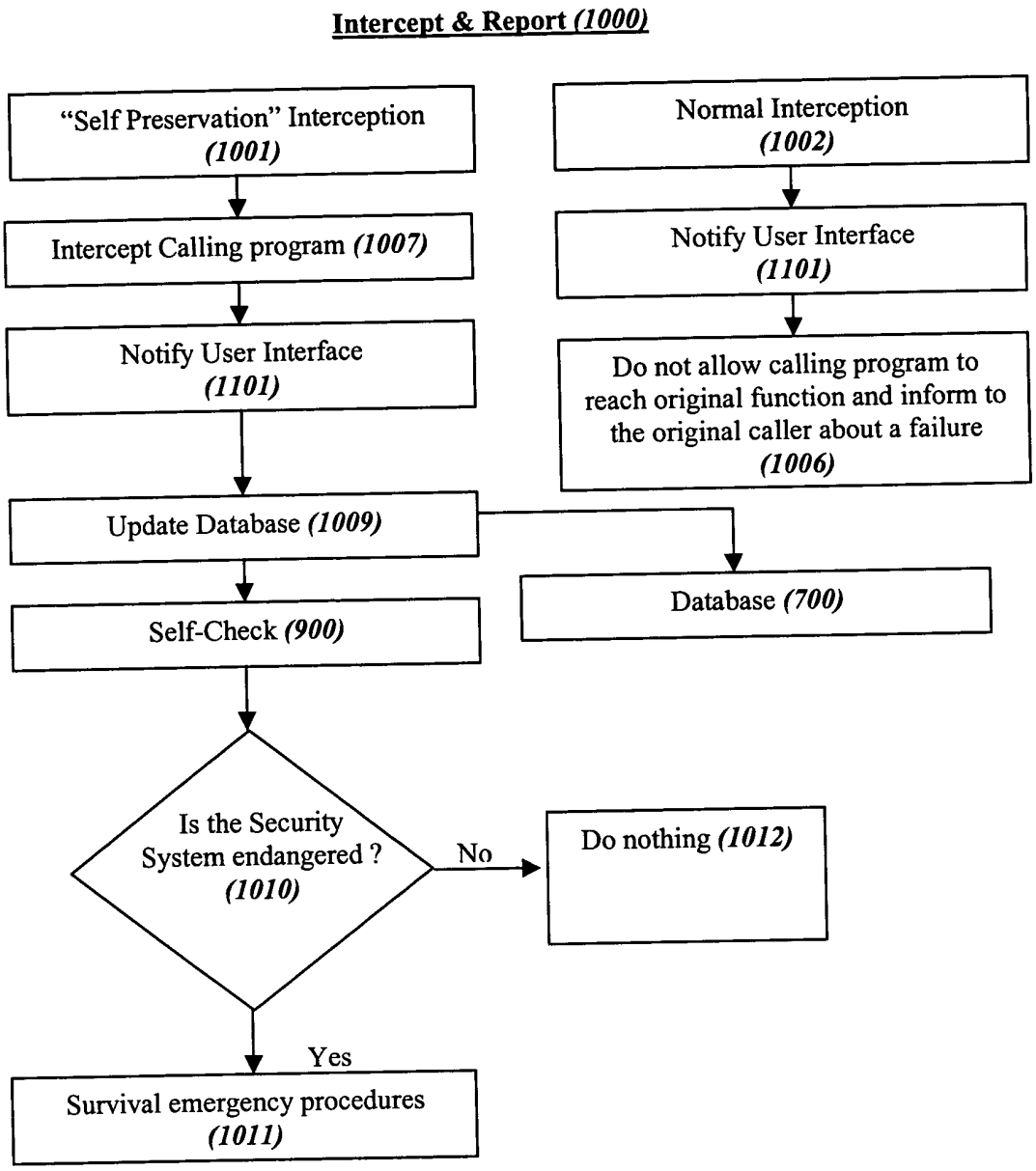

Intercept & Report (1000)
"Self Preservation" Interception (1001)
Normal Interception (1002)
Intercept Calling program (1007)
Notify User Interface (1101)
Notify User Interface (1101)
Do not allow calling program to reach original function and inform to the original caller about a failure (1006)
Update Database (1009)
Database (700)
Self-Check (900)
Is the Security System endangered ? (1010)
No
Do nothing (1012)
Yes
Survival emergency procedures (1011)

Fig 10

Fig. 11

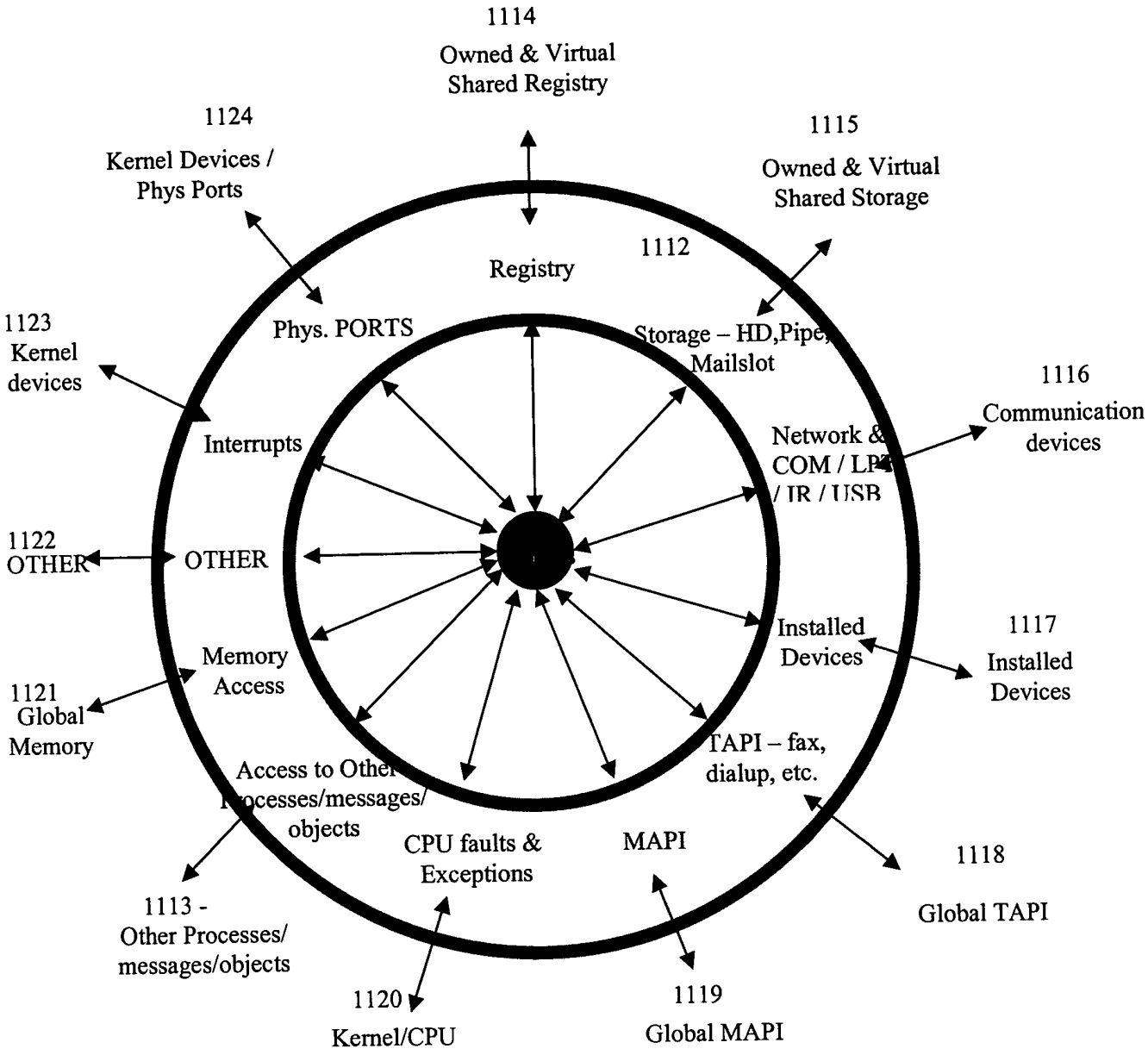

1114
Owned & Virtual
Shared Registry
1124
Kernel Devices /
Phys Ports
1115
Owned & Virtual
Shared Storage
1112
Registry
Phys. PORTS
Storage – HD,Pipe,
Mailslot
1123
Kernel
devices
1116
Communication
devices
Interrupts
Network &
COM / LPT
/ IR / USB
1122
OTHER
OTHER
Installed
Devices
1117
Installed
Devices
Memory
Access
1121
Global
Memory
TAPI – fax,
dialup, etc.
Access to Other
Processes/messages/
objects
CPU faults &
Exceptions
MAPI
1118
Global TAPI
1113 -
Other Processes/
messages/objects
1120
Kernel/CPU
1119
Global MAPI

Fig. 12

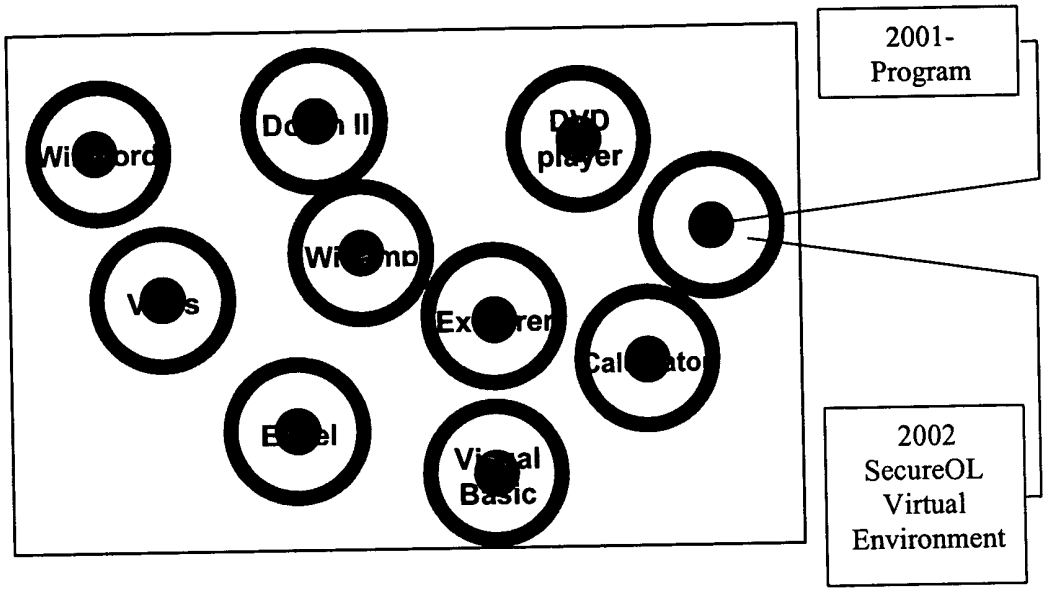

2001-
Program
DVD
player
2002
SecureOL
Virtual
Environment

Fig. 13

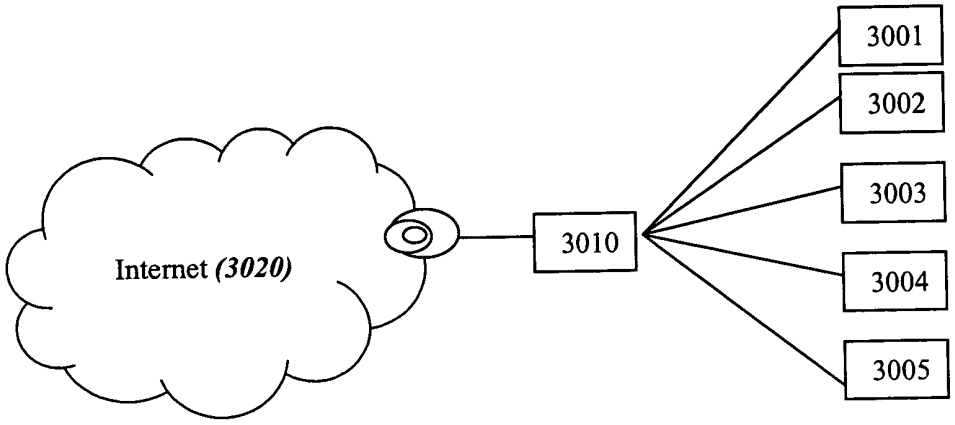
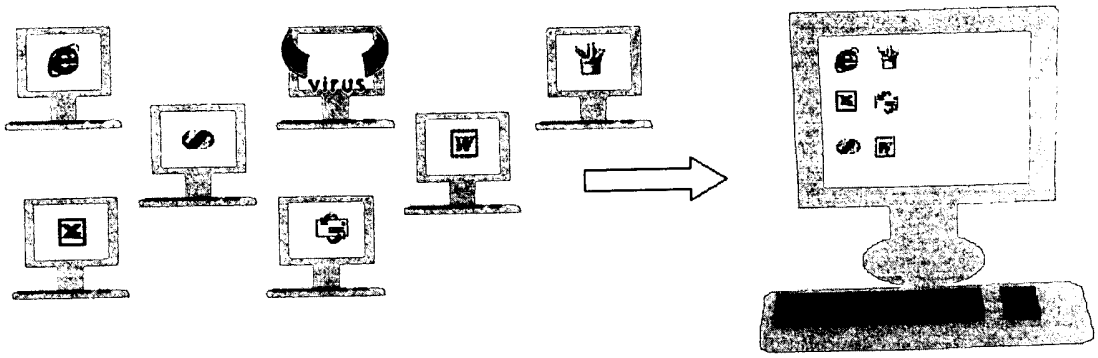

Internet (3020)
3010
3001
3002
3003
3004
3005

Fig. 11a



Physical Virtual environment as seen by the segregated programs (each program by default sees itself alone on the computer, with the resources that it is allowed to see)

Actual appearance as seen by user

Fig. 11b

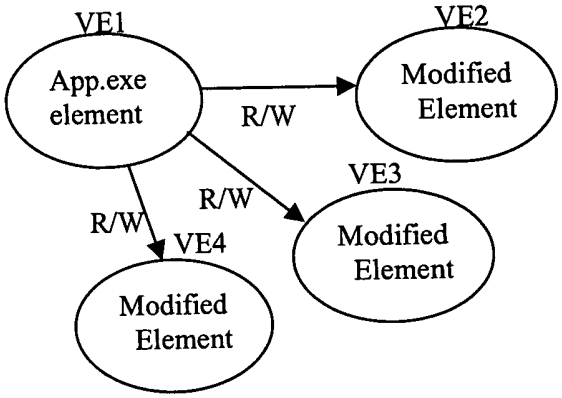


Fig. 11c

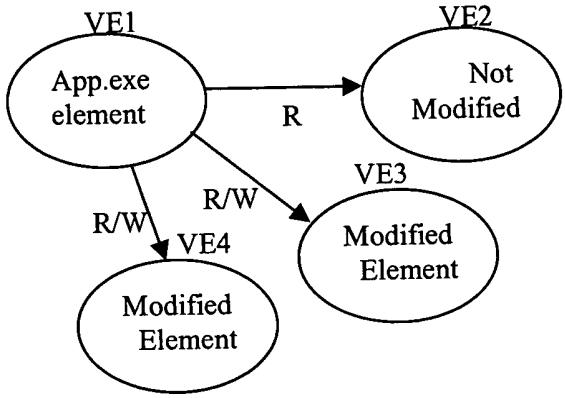


Fig. 11d

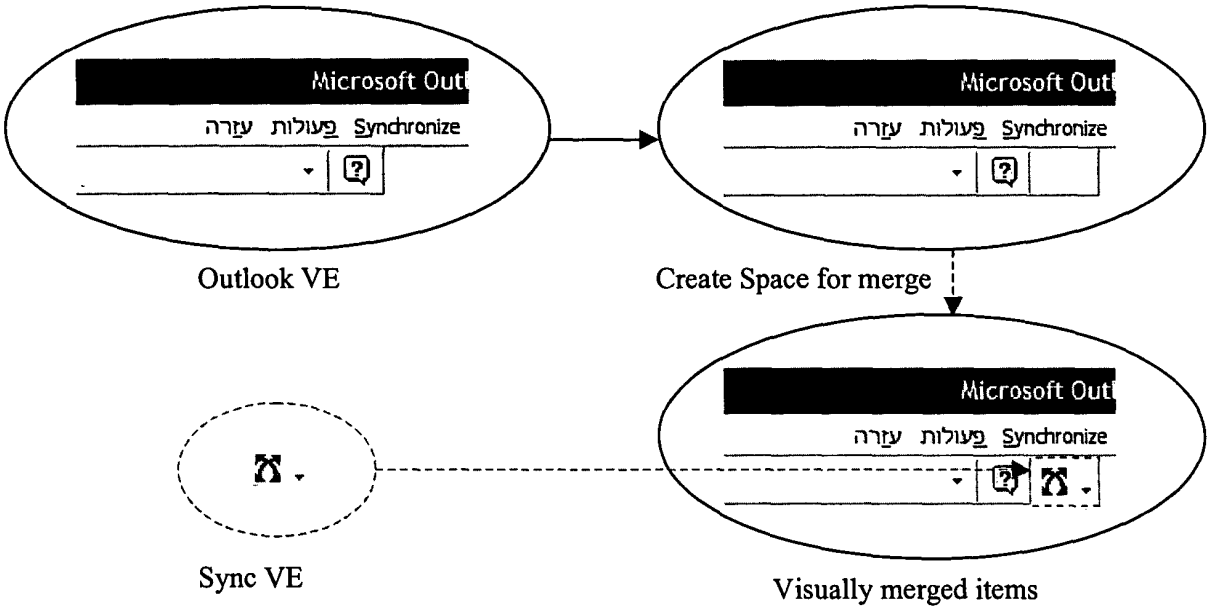
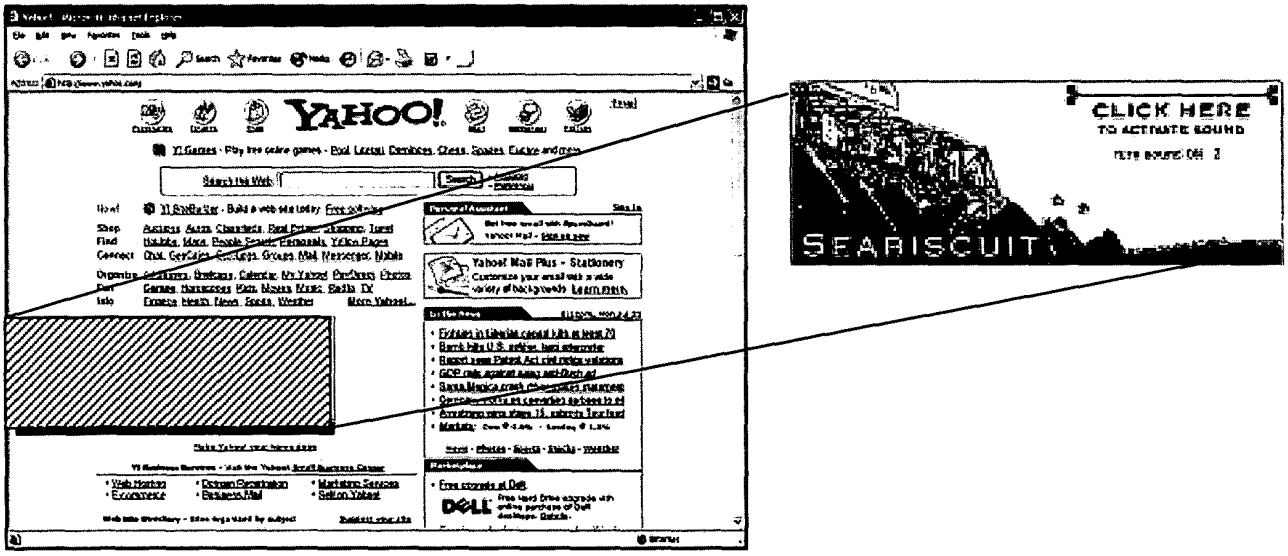



Fig. 11e